1271 Avenue of the Americas
New York, New York 10020-1401
Tel: +1.212.906.1200 Fax: +1.212.751.4864
www.lw.com

LATHAM & WATKINS LLP

FIRM / AFFILIATE OFFICES

Austin	Milan
Beijing	Munich
Boston	New York
Brussels	Orange County
Century City	Paris
Chicago	Riyadh
Dubai	San Diego
Düsseldorf	San Francisco
Frankfurt	Seoul
Hamburg	Silicon Valley
Hong Kong	Singapore
Houston	Tel Aviv
London	Tokyo
Los Angeles	Washington, D.C.
Madrid	

May 28, 2024

VIA ECF

The Honorable Paul A. Engelmayer
Thurgood Marshall United States Courthouse
40 Foley Square
New York, NY 10007

Re: *SEC v. SolarWinds Corp., et al.*, 23-cv-09518

Dear Judge Engelmayer:

Defendants write to reply to the SEC's letter filed on Friday, May 24, 2024, ECF No. 122 ("SEC Ltr."). The SEC's letter does nothing to resolve the glaring contradiction between the AC's allegations concerning the PAN incident and the SEC's belated admission that PAN reported the incident as a "red team exercise," as reflected in incorporated documents.

The SEC initially tries to defend its characterization of the PAN incident as an "attack" on the ground that SolarWinds purportedly "considered the … incident an attack," SEC Ltr. at 1, but in doing so the SEC continues to play fast and loose with the incorporated documents. It misleadingly relies on preliminary internal communications that occurred *before* SolarWinds set up a conference call with PAN on November 5, 2020 to obtain more information about the incident.[1] It was on that November 5 call that PAN explained it was reporting the results of an "exercise" by their "Red Team." Defs.' Ltr. dated May 17, 2024 ("Defs.' Ltr."), Ex. A at 10. The incorporated documents make abundantly clear that, after this fuller briefing, SolarWinds understood PAN's report to be about a red-team exercise, *not* an "attack." *See* SEC Ltr. Ex. C at 7 (November 5 chat message summarizing that PAN explained on the call that the reported activity was part of "a red-team operation"); *id.* at 11 (November 23 message from SolarWinds employee stating: "Given that [the issue being reported] was [an] internal find for them I don't think we should spend more time until they provide us with all information."); *id.* at 13 (November 26 message from SolarWinds employee stating: "Unfortunately they can't make any of their red team available for questions…."); Defs.' Ltr. Ex. A at 3-4 (late November emails in which SolarWinds repeatedly asked PAN if they could speak with "the red team").

---

[1] *See id.* Ex. A at 3 (October 7 message stating that "palo alto [had been] in touch with customer support and *it seems* they had a breach"); *id.* at 2 (October 14 email stating "I don't think this was spun up as an incident yet since [customer support] was still waiting on more info…."); *id.* Ex. B at 1 (October 9 email setting up meeting to discuss a "*potential* issue with Palo Alto like we had with the DOJ"); *id.* Ex. C at 2-6 (internal chat messages from November 5 *before* SolarWinds personnel set up a call with PAN that same day to get more information).

The SEC also seems confused about what a red-team exercise is. It asserts, perplexingly, that "Orion software reaching out to and downloading malicious software *during a red team exercise* is not mutually exclusive with it being an attack." SEC Ltr. at 2 (emphasis added). This assertion makes no sense. Activity conducted "during a red team exercise" *is* "mutually exclusive with it being an attack," because a red-team exercise, by definition, is *not* an actual attack, but an authorized exercise. Indeed, the chat log cited by the SEC reflects that SolarWinds understood that the "downloading of malicious software" PAN was reporting had been done *by a PAN employee* as part of the exercise. *Id.* Ex. C at 7 (stating that PAN had represented that an "[*i*]*nternal employee during a red-team operation* managed to download cobalt strike beacon").[2]

The SEC otherwise tries to backpedal. Having repeatedly characterized the PAN incident as an "attack" in the AC, the SEC now asserts that it is "irrelevant" whether SolarWinds understood it that way, stating that all that matters is "Brown's and SolarWinds' knowledge that the same vulnerability in Orion had been utilized on two different occasions." SEC Ltr. at 2-3. But the SEC's fraud theory concerning the PAN incident has never been about a mere "vulnerability" in Orion. The theory asserted in the AC is that, after the PAN incident, SolarWinds and Mr. Brown knew or should have known that "*an attack*[*er*] was almost surely looking to use Orion in a larger *attack*." AC ¶ 286 (emphasis added). The SEC likewise stated at oral argument that, after the PAN incident, SolarWinds should have disclosed that it "had seen indications that someone [was] looking to use Orion in a broader attack." Oral Arg. Tr. at 61:5-7. This theory—unmistakably premised on the notion that SolarWinds understood the PAN incident to be an "attack"—is utterly untenable given that, as the SEC now concedes, SolarWinds was deliberately led to believe the PAN incident was not in fact an attack. The SEC's abandonment of the theory only confirms that it no longer considers it defensible.

As for the backup theory the SEC seeks to switch to now—that SolarWinds or Mr. Brown knew from the USTP and PAN incidents that Orion had an unidentified vulnerability—that theory is inadequately alleged and could not support a fraud claim regardless. The AC does not allege that SolarWinds ever determined that "the same vulnerability in Orion" was involved in the USTP and PAN incidents; to the contrary, it acknowledges SolarWinds "did not uncover the root cause" of either incident. AC ¶¶ 270, 284. Indeed, the incorporated documents reflect that SolarWinds was not able to form a conclusion even as to "whether there [was] an *unknown* vulnerability at play or not" in the PAN incident—which is incompatible with any allegation that Mr. Brown or others at SolarWinds knew of some vulnerability and sought to conceal it. SEC Ltr. Ex. C at 13 (emphasis added); Defs.' Ltr. Ex A at 3-4. In any event, even if SolarWinds *had* concluded there was a vulnerability in Orion at the time, that would have been entirely consistent with SolarWinds' risk disclosure, which warned that its software was "vulnerable" to attack. Knowledge of a software vulnerability therefore would not have made the disclosure false or misleading, nor would it imply that that anyone at SolarWinds believed it was false or misleading (let alone Mr. Brown,

[2] The PAN employees who spoke with SolarWinds said they were part of PAN's "blue team"—the team assigned to defend PAN's infrastructure in the exercise—and were seeking SolarWinds' help in understanding "the red team's results and what path might have been taken" by the red team in accomplishing its results. Defs.' Ltr. Ex. A at 10.

who is not even alleged to have reviewed the disclosure).

More broadly, the implicit premise of the SEC's position—that companies are obliged to disclose software vulnerabilities in their investor filings—would have absurd consequences. As explained by multiple amici, it is *routine* for software companies to discover security vulnerabilities in their products, and there are well-established industry protocols for disclosing such vulnerabilities to customers—*after* the vulnerability has been fully identified and a patch developed for it. Requiring companies to update their investor filings whenever they discover a vulnerability—let alone an unconfirmed vulnerability—would be not only impractical, but dangerous, as companies would be forced to disclose vulnerabilities before they have been remediated.[3] *See In re Intel Corporation Securities Litigation*, 2019 WL 1427660, at *11 (N. D. Cal. 2019) (rejecting securities fraud claim based on alleged failure to disclose a vulnerability, given, *inter alia*, "the industry practice of keeping the news of security vulnerabilities from the public so hackers cannot take advantage of such flaws before they are fixed" (cleaned up)).

Finally, the SEC cannot take refuge in protestations that the issue of whether the PAN incident was an "attack," or the relevance of that issue to its case, amounts to a "factual dispute." SEC Ltr. at 3.[4] There is no dispute over the facts here. The SEC has repeatedly characterized the PAN report as being about an "attack" and has sought to infer from it that SolarWinds or Mr. Brown knew or should have known that "an attack[er] was almost surely looking to use Orion in a larger attack." Yet the SEC now *admits* that PAN described what it was reporting as a red-team exercise, not an "attack," and the incorporated documents make clear that SolarWinds understood it that way—as the SEC was specifically told during its investigation. The record is thus clear: The SEC knowingly misrepresented the facts and now pretends that it did no wrong. The Court should not indulge these sharp tactics. The SEC's mischaracterizations of the PAN incident in the AC, and the false inferences the SEC seeks to make from them, deserve no credit.

---

[3] *See* Brief of Business Software Alliance, ECF No. 67-1, at 6-7 (explaining that software companies "routinely" find vulnerabilities and release patches for them, and that "indiscriminate public disclosure of a particular vulnerability, or even public awareness that a particular company or product has a serious vulnerability, before that vulnerability is remediated risks alerting malicious actors and providing a blueprint for future attacks"); Brief of CISOs and Cybersecurity Organizations, ECF No. 70-1, at 11-12 & n.48 (explaining that in 2023 alone, more than 28,000 software vulnerabilities were reported by companies in connection with issuing patches for them, and that requiring companies to make "premature" disclosure of vulnerabilities "before mitigation strategies have been carried out" would be "to the benefit of threat actors"); Brief of Former Gov't Officials, ECF No. 73-1, at 12 ("[A] regime that incentivizes early detailed public disclosure of vulnerability information … can actually damage law enforcement investigations, provide a roadmap to aid threat actors, and make companies less safe.").

[4] The SEC uses this argument as an excuse to re-argue points concerning the FedRAMP assessment cited in the AC, going beyond the Court's page limit for letters in the process. SEC Ltr. at 3-4. Because those points exceed the scope of what the SEC was asked to address in its letter, Defendants do not respond to them here.

LATHAM & WATKINS LLP

Respectfully,

/s/ *Serrin Turner*

Serrin Turner
Latham & Watkins LLP
1271 Avenue of the Americas
New York, NY 10020
212-906-1330
serrin.turner@lw.com

Sean M. Berkowitz
Kirsten C. Lee
Latham & Watkins LLP
330 North Wabash Avenue
Suite 2800
Chicago, IL 60611
312-876-7700
sean.berkowitz@lw.com
kirsten.lee@lw.com

Counsel for SolarWinds Corp. and Timothy G. Brown

cc: All Counsel of Record (via ECF)